Purchase and Import a Signed SSL Certificate

FORTINET

1

Overview

STEP 1: Purchase an SSL certificate package from a Certificate Authority (CA)

STEP 2: Generate a Certificate Signing Request (CSR)

STEP 3: Setup the SSL certificate

STEP 4: Import the signed certificate into your FortiGate device

STEP 5: Configure your FortiGate device to use the signed certificate

2

Detailed Steps

Before creating a certificate, you must have a registered domain.

STEP 1: Purchase an SSL certificate package from a Certificate Authority (CA)

SSL certificate packages can be purchased from any CA, such as Comodo, GoDaddy, or GlobalSign.

To purchase a certificate package:

1. Create an account with your chosen vendor, or use the account you used to purchase your domain.
2. Locate the SSL Certificates page.
3. Purchase a basic SSL certificate for domain validation only.

If required, a more secure SSL certificate can be purchased.

After purchasing the certificate, the CA will direct you to setup the certificate so that it can be verified.

If you need to create a CSR, go to STEP 2.

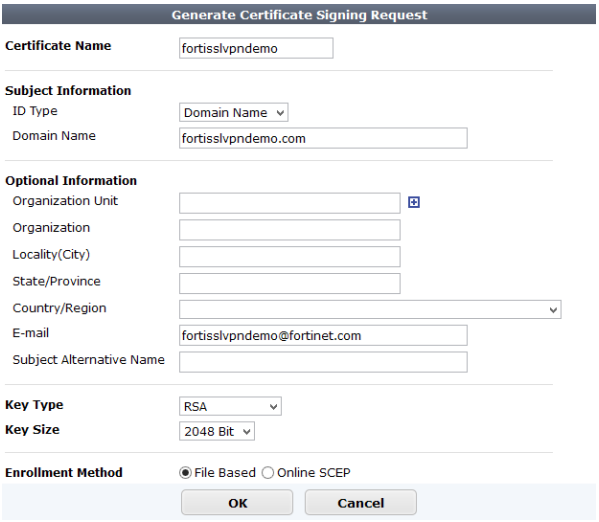
If not, skip to STEP 3.

STEP 2: Generate a Certificate Signing Request (CSR)

Some CAs can auto-generate the CSR during the signing process, or provide tools for creating CSRs, such as GlobalSign's SSL Certificate Signing Request Tool.

If necessary, a CSR can be quickly created from your FortiGate device's GUI.

1. Log in to your FortiGate unit and browse to *System* > *Certificates*.
2. Select *Generate* in the toolbar.



3. Enter the required information in the *Generate Certificate Signing Request* screen:
   - Ensure that the certificate has a unique name.
   - Select *Domain Name* in the *ID Type* field.
   - An email address is required.
   - Ensure that the *Key Size* is set to *2048 Bit*.
   - Set the *Enrollment Method* to *File Based*.

4. Select *OK* to create the CSR.

   The CSR will be added to the certificate list with a status of *PENDING*.

5. Select the new CSR in the *Local Certificates* page and select *Download* to save the CSR to your computer.

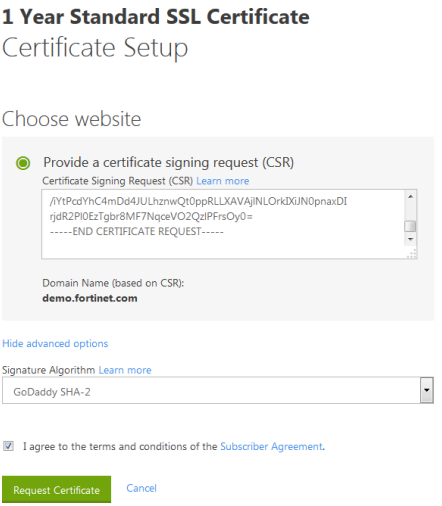
   The CSR file can be opened in any text editor and should resemble the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwgZcxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazEV
MBMGA1UEBxMMTmV3IE5ldyBZb3JrMRcwFQYDVQQKEw5QbGFuZXQgRXhwcmVzczEN
MAsGA1UECxMEQ3JldzEQMA4GA1UEAxMHMC4wLjAuMDEkMCIGCSqGSIb3DQEJARYV
ZnJ5QHBsYW5ldGV4cHJlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAr8yFQ7lmm0MS15zrAPl74HDIrUwVzKNmhYQdGVdM6g+ikOmLM7arStXX
4znafar9IPI/ugAxXdXRy/w6tTzH8W8DsjnrW0EGwXHnujpPNvnsEqtPO5fezje4
lQKJbL1NVUdzM3Finhd+28xPwLkAiL+5rLnTA5zB8onf3R98+PdE+R57xRwawHSr
XhJMSRbpl7IDHW23IL6VEt9FB5bSFQIS5yjslJ8JHcnW+oxnNwngdi1219XI/Kbb
NRrh2QT6S+Ntfz0ZkGVX6fJOY4b+JCa4op41J4Jp6yoZUbkpvEbTXgrz2n6ulwKw
HjKRokWM5SG16haFyM3V+ExUFXbiAwIDAQABoDEwEQYDVR0TMQoTCENBOkZBTFNF
MBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgWgMA0GCSqGSIb3DQEBCwUAA4IB
AQCT+f07oMvDDDIZMKZskInGgCpNlDRELiRgyj0d5Xt31by78G2N15++vfE/Tsdu
dBPrRdA6eAyVgEhBk76JiVUpluQ9dm3TRDpZp/bc+kHc87l2NVSZEpjAKaAeOx5E
0GwQgQKk1RtXO0ABa2b6WxK9aZg/TdHS5ZTMm+jCl6xacgJ8qCt9Nl2DLlWHaXy8
ZO/jI00vpX9FqKVLRq7glpmZgsA7bcZu+NItN0JbARyUL8038URFEiqXzTuR7vX5
LwvNhqqJ9obGAHyFLxn/BsOQA0LQ9jnhWpVasDj3NUS3V6j3+31db92lDplOkbHH
WP2WDWfUp8zx1jYQJpgOjBmW
-----END CERTIFICATE REQUEST-----
```

STEP 3: Setup the SSL certificate

The following instruction use GoDaddy as an example.

1. Immediately after purchasing the certificate, you will be taken to your account page.
2. Find the newly purchased certificate and select *Manage* to open the *Certificate* page.
3. Select *Setup*.
4. If you are using a CSR generated by your FortiGate device:
   a. Open the CSR file in a text editor
   b. Copy the file contents
   c. Paste it into the text box.
5. Select a signature algorithm, read and then agree to the subscriber agreement, then select *Request Certificate*.



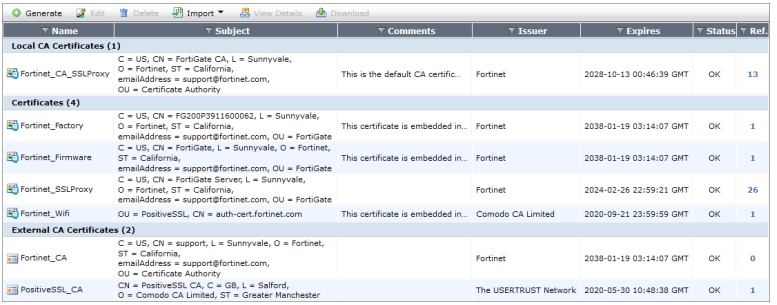
6. The *Certificate Verification* screen opens, the certificate is verified, and you are redirected to the *Certificate Management* screen.
7. Select *Download* to download the signed certificate, as a Zip file, to your computer.
   The server type can be set to *Other*.

STEP 4: Import the signed certificate into your FortiGate device

1. Unzip the file downloaded from the CA.

   There should be two .CRT files: a CA certificate with *bundle* in the file name, and a local certificate.

2. Log in to your FortiGate unit and browse to *System* > *Certificates*.
3. Select *Import* > *Local Certificate* to import the local certificate.



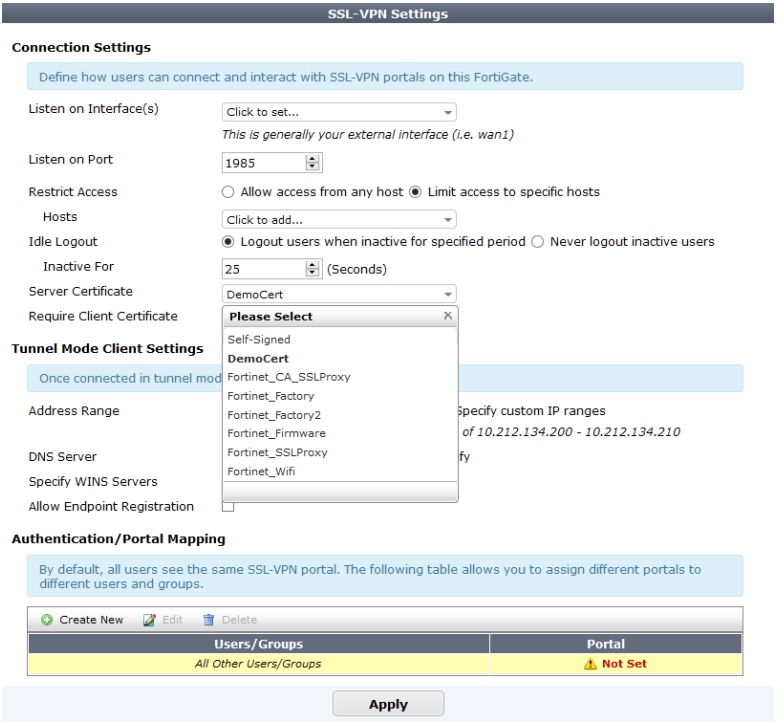
   The status of the certificate will change from *PENDING* to *OK*.

4. Import the CA certificate by selecting *Import* > *CA Certificate*. It will be listed in the *CA Certificates* section of the certificates list.

You can now configure SSL VPN using the signed certificate.

STEP 5: Configure your FortiGate device to use the signed certificate

1. Log in to your FortiGate unit and browse to *VPN* > *SSL* > *Settings*.
2. In the *Connection Settings* section, locate the *Server Certificate* field.



3. Select the new certificate from the drop-down menu.
4. Select *Apply* to configure SSL VPN to use the new certificate.

For more information on configuring SSL VPN, see the SSL VPN Guide, available in the Fortinet Document Library or watch the video available in the Fortinet Video Library.